【140】

氏　名（本籍）	武仲正彦（兵庫県）
学位の種類	博　士（工　学）
学位記番号	博甲第4954号
学位授与年月日	平成21年3月25日
学位授与の要件	学位規則第4条第1項該当
審査研究科	システム情報工学研究科
学位論文題目	**実装を考慮した暗号解析手法に関する研究**

主　査	筑波大学教授	理学博士	井田哲雄
副　査	筑波大学教授	工学博士	岡本栄司
副　査	筑波大学教授	博士（工学）	李　頡
副　査	筑波大学准教授	博士（工学）	亀山幸義
副　査	筑波大学准教授	博士（工学）	満保雅浩

論文の内容の要旨

本論文は，安全な情報社会を実現する上で欠かすことのできない暗号技術の安全性に関して，暗号の実装を考慮した解析を行うことの重要性を明らかにした論文である。第1章は本研究への序論であり，研究背景を概観した後，次の2つの研究目的を述べている。すなわち，暗号技術に対する実装を中心とした具体的な解析手法を考案すること，及び，第2章で示す4つの視点から暗号技術を分類することにより暗号技術の安全性評価に必要な解析を包括的に可能とすることである。

第2章は準備として，本論文で共通に使用する用語や概念，並びに，関連研究について説明を行っている。暗号技術を，安全性の根拠となる暗号プリミティブとその動作方法を規定する暗号スキーム，及び，それらの仕様と実装という項目を組み合わせることにより得られる4つの視点から分類している。

これら4つの視点の内，3つにおいて，具体的な暗号解析を示している。まず第3章では，暗号プリミティブの仕様に対する解析の一環として，共通鍵ブロック暗号RC6のx^2攻撃に係わるモデル化を述べている。これにより，従来，実験的な解析しか行われてこなかったRC6におけるx^2攻撃に対する詳細なセキュリティ評価を可能とした。次に第4章では，暗号プリミティブの実装の解析手法として，Address-bit DPAと呼ばれる解析手法とその拡張を述べている。この拡張により，これまでAddress-bit DPAを用いた攻撃への対策の必要性が認識されていなかった公開鍵暗号プリミティブOK-ECCの実装解析が可能となった。更に第5章では，暗号スキームの実装に対する解析手法として，Bleichenbacher攻撃と呼ばれる署名偽造手法を拡張し，その拡張手法を効果的に適用することで，実運用されているタイムスタンプの偽造方法を示している。

第6章では，以上の3つの暗号解析による安全性評価を比較し，その社会的な影響を分析することで，実装を考慮した暗号解析の重要性を主張している。第7章は結論であり，全体のまとめを行うとともに，今後の研究の展望を記している。

審 査 の 結 果 の 要 旨

本論文では，暗号技術を暗号プリミティブと暗号スキームに分類し，それに仕様と実装を与えることで得られる 4 つの視点から暗号技術を考察し，暗号技術の安全性を論じている。既存の暗号の研究開発者でさえも見逃しがちな，実装に関する解析を含む各種の解析手法の存在に包括的に焦点を当てており，より安全性の高い暗号の研究開発につながる重要な知見を得ている。提示されている解析方法は，当該分野の関連研究において多数引用される，運用されているシステムに適用される等，本研究の社会的波及効果が既に見られる。以上から，本論文は，情報セキュリティ分野の学術の発展に十分に寄与するものと判断する。

よって，著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。